IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

Chris Schulte, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T Inc. and AT&T Mobility LLC. Defendants.	Case No. 24-CV- 07818 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Chris Schulte, ("Schulte" or "Plaintiff"), individually and on behalf of all others similarly situated, bring this action against AT&T Mobility LLC ("Mobility) and AT&T, Inc. (collectively, "AT&T" or "Defendants" or the "Company"), based on his personal knowledge and the investigation of counsel and allege as follows:

INTRODUCTION

1. This is a class action brought by Plaintiff on behalf of himself and the other similarly situated persons whose personal information was acquired and/or accessed by unauthorized persons in the data breach that AT&T describes through its filing with the Securities and Exchange Commission (the "SEC") dated July 12, 2024 (the "2024 Cellular Data Breach").

2. Upon information and belief, Plaintiff and the proposed class members first learned of the 2024 Cellular Data Breach through news outlets reporting the breach on July 12, 2024.

3. The 2024 Cellular Data Breach has been estimated to impact **nearly all** of AT&T's over 241.5 million wireless customers and customers of mobile virtual network operators ("MVNO") who used AT&T's wireless networks between May 1, 2022 and October 31, 2022, plus every person with whom an AT&T customer called or texted during that time period, including customers of other wireless networks, plus certain customers who used AT&T's wireless networks on January 2, 2023.

4. The 2024 Cellular Data Breach affected individuals whose information was stored on AT&T's servers in multiple states.

5. AT&T provides wireless voice, messaging, and data services in the United States, including Puerto Rico and the U.S. Virgin Islands.

6. The Company operates one of the largest wireless networks in the U.S. market, with over 114 million Mobility customers.

7. Plaintiff and other members of the proposed class were required, as current and former customers of AT&T, to provide AT&T with sensitive personal information to apply for and/or receive wireless voice, messaging, and data services. AT&T assured Plaintiff and other members of the proposed class that their personal information would be kept safe from unauthorized access.

8. AT&T states that it takes cybersecurity very seriously and privacy is a "fundamental commitment" at AT&T. Despite this, AT&T failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the sensitive and

personal identifying information of Plaintiff and the proposed class. Moreover, AT&T betrayed the trust of Plaintiff and other members of the proposed class by failing to properly safeguard and protect their sensitive personal information, and by enabling cybercriminals to acquire and/or access it.

9. Upon information and belief, the data subject to the 2024 Cellular Data Breach was sensitive personal information that was unencrypted and unredacted and compromised by AT&T's failure to take proper safeguards of the information.

10. AT&T's failure to secure its users' sensitive personal information is particularly egregious given the known dangers of security hacks and data breaches generally, and AT&T's own numerous, significant, and serious prior data breaches.

11. Plaintiff brings this class action against AT&T for its failure to properly secure and safeguard the sensitive and personally identifiable information of Plaintiff and the members of the proposed class stored within AT&T's information network, including, their telephone numbers and the numbers of those with whom they called and texted, the number of times they interacted with those parties and the call duration of their telephonic communications, and in some cases, geolocating information (this type of information, inter alia, being hereafter referred to, collectively, as "personally identifiable information" or "PII").

12. AT&T disregarded the rights of Plaintiff and the other members of the proposed class by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and other members of the proposed class was safeguarded.

13. Specifically, AT&T ignored the rights of Plaintiff and other members of the proposed class by, inter alia, intentionally, willfully, recklessly or negligently failing to:

(1) ensure the security and confidentiality of consumer records and PII; (2) protect against anticipated threats or hazards to the security or integrity of consumer records and PII; (3) protect against unauthorized access to or use of consumer records or PII that could result in substantial harm or inconvenience to any current or former customer; (4) implement or maintain policies and procedures that adequately secured consumers' records and PII; (5) sufficiently monitor, audit and update its cybersecurity procedures and patch maintenance; and (6) timely detect the 2024 Cellular Data Breach, mitigate harm, and notify consumers of the 2024 Cellular Data Breach. As a result, the PII of Plaintiff and other members of the proposed class was compromised through disclosure to and access by one or more unknown and unauthorized third parties.

14. Plaintiff and other members of the proposed class have suffered injury because of AT&T's conduct. These injuries include: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2024 Cellular Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiff's and the prospective class members' PII in their continued possession; (g) future costs in terms of time, effort, and money that will be expended as a result of the 2024 Cellular Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (h) the diminished value of Plaintiff's

and the prospective class members' PII; (i) the diminished value of AT&T's services Plaintiff and other members of the proposed class paid for and received; and/or (j) the actual and attempted sale of Plaintiff's and the prospective class members' PII on the dark web.

15. In addition to remedying the harms suffered because of the 2024 Cellular Data Breach, Plaintiff and the millions of customers similarly situated also have a significant interest in preventing additional data breaches, as their PII remains in AT&T's possession without adequate protection.

16. Plaintiff brings this action on behalf of all persons whose PII was compromised because of AT&T's failure to: (i) adequately protect the PII of Plaintiff and other members of the proposed class; (ii) warn Plaintiff and other members of the proposed class of these inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. AT&T's conduct amounts to negligence and violates federal and state statutes.

17. Plaintiff, for himself and for others similarly situated current and former customers of AT&T impacted by the 2024 Cellular Data Breach, seek actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses. Plaintiff also seek declaratory and injunctive relief, including significant improvements to AT&T's data security systems and protocols (which have been the subject of multiple recent data breaches), future annual audits, AT&T-funded long-term credit monitoring services, and any other remedies the Court deems necessary and proper.

THE PARTIES

18. Plaintiff Chris Schulte is and has been a customer of, and received wireless voice, messaging, and data services from, AT&T.

19. The reports regarding the breadth and severity of the 2024 Cellular Data Breach and AT&T's disclosures concerning the number and class of consumers affected indicate, upon information and belief, that Plaintiff and his data have been impacted.

20. To receive wireless voice, messaging, and data services from AT&T, Plaintiff were required to provide AT&T with sensitive PII. Plaintiff's PII was within the possession and control of AT&T at the time of the 2024 Cellular Data Breach.

21. Plaintiff brings this action on behalf of himself, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

22. Defendant AT&T, Inc. is a Delaware corporation with its principal place of business located in Dallas, Texas and is incorporated under the laws of the State of Delaware.

23. AT&T Mobility LLC is a Delaware limited liability company with its principal place of business in Brookhaven, Georgia. Mobility is a wholly owned subsidiary of AT&T.

24. AT&T operates one of the largest wireless networks in the U.S. market with over 242 million customers.

25. AT&T has access to enormous resources. In 2023, AT&T reported total revenues of more than $122.4 billion – with over $118 million of the aforementioned coming from Mobility and other communications business segments – and net income of more than $23 billion.

JURISDICTION AND VENUE

26. This Court has diversity jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332. This is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members

in the proposed class, and upon information and belief, at least one other member of the proposed class is a citizen of a state different from Defendants.

27. This Court has personal jurisdiction over Defendants because: one or both of the Defendants routinely conduct business in New Jersey, and has sufficient minimum contacts in New Jersey, has intentionally availed itself or themselves of this jurisdiction by marketing and selling products and services in New Jersey and the events that give rise to Plaintiff's claims occurred in part in this District.

28. Venue is proper in this District under 28 U.S.C. § 1391 because, inter alia: (a) Defendant conducts substantial business in this District, (b) Defendant directed its services at residents in this District, and (c) events that give rise to this action took place in this District.

FACTUAL ALLEGATIONS

A. AT&T's Collects, Stores and Profits from Consumer Information and Promises to Keep it Secure

29. AT&T cites that it is different from its competitors, touting a legacy of "connecting people" by "powering the world's first phone call in 1876, [. . .] helping NASA call a man on the moon 240,000 miles away, and creating the lifesaving 911 emergency system we all depend on." AT&T calls itself the carrier which "connect[s] people for good."

30. AT&T offers numerous types of cellular plans, including unlimited plans, prepaid plans, plans for first responders, plans for the military and veterans, and more.

31. In the course of its business, AT&T collects, maintains, and profits from the PII of millions of U.S. consumers. AT&T also maintains this PII for former customers for an indefinite period of time.

32. In the course of providing telecommunications services, AT&T requires customers to provide certain private information. Among other personal information, AT&T collects the following, according to its Privacy Notice:

> **Account Information:** You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information.
>
> **Equipment Information:** We collect information about equipment on our network like the type of device you use, device ID, and phone number.
>
> **Network Performance:** We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.
>
> **Location Information:** Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.
>
> **Web Browsing and App Information:** We automatically collect a variety of information which may include time spent on websites or apps, website and addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.
>
> **Biometric Information:** Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice.

33. The Privacy Notice applies to AT&T products and services including wireless, voice, and internet.

34. AT&T's Privacy Policy is available on its website and provides customers with detailed promises regarding the treatment of their PII, including how AT&T uses customers' data, which includes for its own benefit and profit.

35. Among other things, AT&T states that it uses customers' personal data to "understand which additional products and services may interest you and others"; and to "[d]esign and deliver advertising, marketing and promotional campaigns to you and others."

36. AT&T further states that customers' PII "can be used to analyze and track online activity or deliver ads and content tailored to your interests." AT&T also "may share information with affiliates and other companies to deliver our ads and marketing or to assess their effectiveness."

37. In addition, AT&T partners with non-AT&T companies and "may provide aggregate metrics reports to that business about how the Wi-Fi is being used, such as aggregated location and web browsing data."

38. According to AT&T, when it shares customer data, it requires its affiliates to "follow [AT&T's] Privacy Notice regarding your info, not just their own policy." Additionally, AT&T "require[s] them to use it only for the intended purpose and to protect it consistent with this notice."

39. Given the highly sensitive and personal nature of the information it collects, handles and mandates customers share, AT&T pledges to uphold the confidentiality and security of PII. Thus AT&T's Privacy Policy further tells customers, that it "work[s] hard to safeguard your information using technology controls and organizational controls. We protect our

computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information."

40. In acquiring, collecting, utilizing and benefitting from the PII of Plaintiff and the prospective class members, AT&T undertook legal and equitable obligations. It knew or should have known that it had a responsibility to safeguard the PII of Plaintiff and the prospective class members.

41. As discussed herein, however, AT&T failed to comply with its promises to protect Plaintiff's PII and its legal obligations to do the same.

B. Despite Its Promises, AT&T Failed to Protect the Sensitive PII of Plaintiff and Others

42. At the same time AT&T collected, stored, and profited from Plaintiff's PII—and was actively communicating to consumers that "[w]e work hard to safeguard your information"—it suffered the massive data breach at issue in this lawsuit, which is only one of many AT&T has experienced over the past several years and the ***second*** massive data breach AT&T has announced in the past several months.

43. On July 12, 2024, AT&T announced that it had been hacked. According to its July 12, 2024 SEC Form 8-K filing (the "Form 8k Filing), on April 19, 2024, *only after cybercriminals* (referenced herein as the "Cybercriminal") *boldly announced the crime they had successfully executed* AT&T learned that the Cybercriminal unlawfully accessed and copied AT&T call logs. According to AT&T, the data was illegally downloaded from its workspace on a third-party cloud platform, Snowflake.

44. Despite allegedly activating its incident response process to investigate, the Cybercriminal was able to infiltrate AT&T's systems from April 14, 2024 through April 25, 2024. Ultimately, AT&T discovered that the Cybercriminal accessed an AT&T workspace on a third-party cloud platform and exfiltrated files "containing AT&T records of customer call and text interactions that occurred between *approximately* May 1 and October 31, 2022, as well as on January 2, 2023." (Emphasis added).

45. AT&T further stated that the stolen records identified "the telephone numbers with which an AT&T or MVNO wireless number interacted during these periods, including telephone numbers of AT&T customers and customers of other carriers, counts of those interactions, and aggregate call durations for a day or month." Further, for certain of those records, "one or more cell site identification number(s) are also included."

46. It its 8-K Filing, AT&T conceded that while the data did not include customer names, "*there are <u>often</u> ways, <u>using publicly available online tools</u>*, to find the name associated with a specific telephone number." (Emphasis added). Inexplicably, however, AT&T also claimed that the data did not contain personally identifiable information.

C. <u>AT&T Compounds Its Failures By Providing Inadequate Notice</u>

47. On July 12, 2024, AT&T posted an article entitled "Unlawful access of customer data" on its website at https://www.att.com/support/article/my-account/000102979?source=EPcc000000000000U (last accessed July 16, 2024) (the "Website Post"). The Website Post contains the same information as the 8-K Filing.

48. As of the date of this filing, there is no notice of the breach on the AT&T customer "landing page," and there is no link to the Website Post on that page. *See*

https://www.att.com/log-in/?msockid=1a15516aad2b609b17224378ac0761c8 (last accessed July 16 2024).

49. Upon information and belief, to date, AT&T has not directly notified Plaintiff or other customers about the 2024 Cellular Data Breach.

50. AT&T's inadequate notice has compounded the harm suffered by Plaintiff and prospective class, by failing to timely provide victims of the 2024 Cellular Data Breach with the critical details necessary to protect themselves.

D. Plaintiff's Experience

51. Plaintiff required and did provide his PII in connection with obtaining services provided by AT&T. Plaintiff at all times relevant hereto is and has been a customer of AT&T.

52. Plaintiff takes measures to protect his PII and is careful about sharing his PII.

53. Plaintiff learned that his PII was implicated by the 2024 Cellular Data Breach, but did not first learn of the same from AT&T. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff already has suffered injury and remains at a substantial and imminent risk of future harm.

54. AT&T knew it was storing sensitive PII and that, as a result, its systems and Plaintiff's and the prospective class members' PII would be an attractive target for cybercriminals.

E. AT&T Has a History of Repeated Data Breaches

55. AT&T is well aware of the risks of storing customer data, including through its third-party vendors, because, among other reasons, it has suffered multiple cyberattacks. Among other unlawful intrusions into its systems, AT&T experienced a data breach in January 2023 that exposed nine million customer records. In May 2023, a security researcher disclosed a

vulnerability in AT&T's systems that had allowed anyone with a target ZIP code and phone number to perform an account takeover through the AT&T website. Moreover, in March 2024, AT&T announced that it experienced a massive cyberattack that affected over 70 million current and former account holders.

56. AT&T could have prevented this latest data breach by properly encrypting or otherwise protecting its equipment and network files containing PII.

57. Despite widespread industry warnings, and its own cyberattacks, AT&T failed to implement and use reasonable security procedures and practices to protect the PII of Plaintiff and members of the prospective class.

58. The 2024 Cellular Data Breach highlights the inadequacies inherent in AT&T's security systems, its network monitoring procedures and security training protocols. Had AT&T properly monitored its cybersecurity systems, implemented sufficient monitoring procedures and training protocol for its employees – particularly given that it suffered a breach about which it gave the public the month prior to the 2024 Cellular Data Breach – it would have prevented the 2024 Cellular Data Breach, detected it, and/or have prevented the hackers from accessing the stolen PII.

59. Further, AT&T's failure to timely notify Plaintiff and other victims of the 2024 Cellular Data Breach that their PII had been misappropriated precluded them from taking immediate meaningful steps to safeguard their identities prior to the dissemination of their PII.

60. AT&T's delayed response has only worsened the consequences of the 2024 Cellular Data Breach brought on by its systemic cybersecurity failures.

F. Data Breaches Pose Significant Threats to Consumers

61. Data breaches have become a serious threat that, in the absence of adequate safeguards, can expose personal data to bad actors and lead to considerable costs to consumers.

62. Cybercrime is slated to cost the world $10.5 trillion annually by 2025.

63. Identity theft is the most common consequence of data breaches to consumers. Consequently, thieves find PII an invaluable commodity, it is the most frequent target of hackers, and it is for sale on the Dark Web.

64. Further, there may be a time lag between when Plaintiff's and the prospective class members' PII was stolen and when it is used. Malicious actors often wait months or even years to use the PII obtained in data breaches, as victims often become less diligent in monitoring their accounts after a significant period has passed. Further, beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.

65. Despite the prevalence of public announcements of data breach and data security compromises, the known risks posed by compromises of PII, and its own history of security breaches, AT&T failed to take proper action to protect the PII of Plaintiff and the prospective class. As a result, the injuries to Plaintiff and the prospective class were directly and proximately caused by AT&T's failure to implement or maintain adequate data security measures for its customers.

66. The National Institute of Standards and Technology (the "NIST") regularly provides guidance and advice on the various cybersecurity practices organizations should employ to maintain the security of consumer PII stored in their servers in the form of a cybersecurity

framework consisting of five major functions of cybersecurity organizations must engage in to maintain sufficient security standards.

67. Among more detailed standards, the NIST Cybersecurity Framework provides the following guidance: a. Identify the organization's asset management, business environment, governance, risk assessment, risk management strategy, and supply chain risk management; b. Protect through identity management and access control, personnel awareness and training, implementing data security, implementing information protection processes and procedures, maintenance, and protective technology; c. Detect anomalies and events through continuous security monitoring to identify cybersecurity events and verify the effectiveness of protective measures, and through detection processes that are maintained and tested to ensure awareness of anomalous events. d. Respond with a response plan, communication with internal and external stakeholders, analysis to ensure effective response and support recovery activities, mitigation activities to prevent expansion of the event and effects, and improvements to the response plan for future cybersecurity events; e. Recover by executing recovery plans and procedures to ensure restoration of affected systems or assets, improving upon recovery planning and processes by incorporating lessons learned, and communicating recovery activities to internal and external stakeholders as well as executive and management teams.

68. Further, the FTC provides an overarching data security plan built on similar principles to the NIST guidance detailed above. According to the FTC, a sound data security plan is built on 5 key principles: a. Take Stock. Know what personal information is on your computers. b. Scale Down. Keep only what is needed for business. c. Lock It. Protect the information that is kept. d. Pitch it. Properly dispose of information that is no longer needed. e. Plan Ahead. Create a plan to respond to security incidents.

69. The FTC provides more specific guidance regarding security including the following directives: a. Identify the computers or servers where sensitive personal information is stored; b. Assess the vulnerability of computers and servers to commonly known or reasonably foreseeable attacks; c. Implement policies to update and correct and security problems; d. Only store consumer data that is essential for conducting business purposes; e. Encrypt sensitive information sent to third parties over public networks; f. Encrypt sensitive information stored on the computer network, laptops, or portable storage devices used by employees; g. Regularly run up-to-date anti-malware programs on individual computers and on servers on the network; h. Use Transport Layer Security (TLS) encryption or another secure connection to protects when receiving or transmitting personal identifying information; i. Control access to sensitive information by requiring "strong" passwords; j. Require and implement multi-factor authentication; k. Caution against transmitting sensitive personally identifying data via email; l. Implement a firewall for protection from internet hackers. Further, determine whether a "border" firewall is needed where the network connects to the internet; m. Encrypt information sent over wireless networks; n. Only use wireless routers with Wi-Fi Protected Access 2 (WPA2) capability and devices that support WPA2; o. Maintain central logs of security-related information to monitor activity and respond to possible attacks; p. Utilize intrusion detection systems; q. Monitor incoming traffic for suspicious behavior and/or large amounts of transmitted data; r. Monitor outgoing traffic for suspicious behavior and/or large amounts of transmitted data; s. Train employees to recognize security threats; t. Before outsourcing business functions investigate the third-party company's data security to ensure reasonable security measures; u. Limit employee and vendor access to sensitive data; and v. Utilize industry-tested methods for security.

70. AT&T failed to comply with one or more of these standards.

G. AT&T Has Harmed Plaintiff and the Prospective Class Members

71. To date, Defendants have failed to adequately protect Plaintiff and the prospective class members or to compensate them for their injuries sustained in the 2024 Cellular Data Breach. As a result, due to the actual and imminent risk of identity theft, Plaintiff and the prospective class members must, "remain vigilant" and monitor their financial and other accounts for the foreseeable future, and possibly the rest of their lives, to mitigate the risk of identity theft or other harm.

72. Plaintiff and the prospective class members have spent, and must continue to spend additional time in the future, on a variety of prudent actions, such as placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and/or filing police reports.

73. Furthermore, Defendants' poor data security deprived Plaintiff and the prospective class members of the benefit of their bargain. When agreeing to pay for AT&T's services, Plaintiff and the prospective class members as AT&T's customers understood and expected that they were paying for services and data security, when in fact, AT&T did not provide the expected and promised data security. Accordingly, Plaintiff and the prospective class members received services of lesser value than they reasonably expected and paid for.

74. As a result of Defendants' ineffective and inadequate data security and retention measures, the 2024 Cellular Data Breach, and the imminent risk of identity theft, Plaintiff and the prospective class members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial costs incurred in mitigating the materialized risk and

imminent threat of identity theft; (c) loss of time and productivity incurred in mitigating the materialized risk and imminent threat and risk of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of the benefit of their bargain; (h) deprivation of the value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiff's and the prospective class members' personal sensitive information.

75. Plaintiff and the prospective class members provided their personal information to AT&T and/or its affiliates in conjunction with the product and services they obtained. As part of their involvement with AT&T, Plaintiff and the prospective class members entrusted their PII, and other confidential and sensitive information such as name, address, phone number, financial account information, and other personally identifiable information to AT&T and its affiliates with the reasonable expectation and understanding that they would at a minimum take standard industry precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related thereto. They would not have permitted their PII to be given to AT&T had they known it would not take reasonable steps to safeguard their PII.

76. As a result of the 2024 Cellular Data Breach, Plaintiff and the prospective class members have or will make reasonable efforts to mitigate the impact of the 2024 Cellular Data Breach, including but not limited to, researching the 2024 Cellular Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

77. Plaintiff and the prospective class members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) damage to and the diminution in value of their PII, a form of property Defendant obtained from Plaintiffs; (b) violation of their privacy rights; (c) theft of their PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

CLASS ACTION ALLEGATIONS

78. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following class (collectively, the "Class"):

> All persons residing in the United States whose personal information was acquired or accessed by unauthorized individuals as a result of the breach of AT&T information system(s) that was reported in its July 12, 2024 8-K Filing.

79. The following individuals and entities are excluded from the proposed Class: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

81. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable. Upon information and belief, the total number of Class members is in

the millions of individuals. Membership in the classes will be determined by analysis of Defendants' records.

82. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class ("Class Members") were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class Member because Plaintiff and each Class Member had their PII compromised in the same way by the same conduct of Defendants.

83. Adequacy: Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class that he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

84. A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

85. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- Whether Defendant engaged in the wrongful conduct alleged herein;
- Whether Defendants had a duty not to disclose the Plaintiff's and Class members' PII to unauthorized third parties;
- Whether Defendants failed to adequately safeguard Plaintiff's and Class members' PII;
- Whether Defendants owed a duty to Plaintiff and the Class to adequately protect their PII, and whether Defendants breached this duty;
- Whether Defendants' systems, networks, and data security practices used to protect Plaintiff's and Class Members' PII violated the FTC Act, and/or Defendants' other duties discussed herein;
- Whether Defendant knew or should have known that their computer and network security systems were vulnerable to a data breach;
- Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the 2024 Cellular Data Breach;
- Whether Defendants breached contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;
- When Defendants actually learned of the 2024 Cellular Data Breach;
- Whether Defendants failed to adequately respond to the 2024 Cellular Data Breach, including failing to investigate it diligently and notify affected individuals

in the most expeditious time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

- Whether Defendants fully and adequately addressed and fixed its systems' vulnerabilities which permitted the 2024 Cellular Data Breach to occur;
- Whether Defendants engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;
- Whether Defendant continues to breach duties to Plaintiff and the Class;
- Whether Plaintiff and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;
- Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;
- Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members and the public;
- Whether Defendants' actions alleged herein constitute gross negligence; and
- Whether Plaintiff and Class Members are entitled to punitive damages.

86. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants 'conduct with respect to the Class in its entirety, not on facts or law applicable only to the Plaintiff.

87. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to act unlawfully as set forth in this Complaint.

CLAIMS FOR RELIEF

Count I - Negligence

88. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

89. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty of care, inter alia, to act with reasonable care to secure and safeguard the PII of Plaintiff and Class Members and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and Class members in its computer systems and on its networks.

90. In order to use Defendants' goods and services, Plaintiff and Class Members were obligated to provide Defendants with their PII, including, their names, addresses, telephone number and other sensitive personal information, depending upon the product or service.

91. Defendants' duties, Defendants were expected to:

- Exercise reasonable care in obtaining, retaining, securing, and protecting PII in their possession;
- Protect Plaintiff's and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;
- Exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' PII was adequately secured

from impermissible access, viewing, release, disclosure, and publication, including patch maintenance;

- Adequately monitor, audit, and update the security of its networks and systems including patch maintenance;
- Implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers;
- Recognize in a timely manner that Plaintiff's and other Class Members' PII had been compromised;
- Promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected; and
- Timely detect and mitigate the 2024 Cellular Data Breach.

92. Defendants knew that the PII of Plaintiff and Class Members was private and confidential and should be protected as private and confidential; therefore, Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

93. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

94. Defendants knew, or should have known, that cyber criminals routinely target large corporations through cyberattacks to steal sensitive personal information.

95. Defendants knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

96. Because Defendants knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class Members, AT&T had a duty to adequately protect its data systems and the PII contained thereon.

97. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the 2024 Cellular Data Breach. These "independent duties" are untethered to any contract between Defendants and Plaintiff and Class Members.

98. Plaintiff's and Class Members' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect its systems and the PII it stored on them from attack.

99. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and Class Members had no ability to protect their PII that was in Defendants 'possession. As such, a special relationship existed between Defendants and Plaintiff and Class Members.

100. AT&T breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class Members.

101. AT&T breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

- Failing to exercise reasonable care in obtaining, retaining, securing, and protecting PII in its possession;

- Failing to protect Plaintiff's and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;
- Failing to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiff's and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication;
- Failing to adequately train its employees to not store PII longer than absolutely necessary;
- Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;
- Failing to implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers;
- Failing to adhere to the applicable industry standards for cybersecurity and exercise reasonable care, thus leaving Plaintiff's and the Class Members' PII vulnerable to theft;
- Failing to heed industry warnings and alerts to provide sufficient safeguards to protect Plaintiff's and Class Members' PII in the face of known risks of hackers and theft; and
- Failing to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

102. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they can take

appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

103. AT&T breached its duty to notify Plaintiff and Class Members of the unauthorized access by failing to notify Plaintiff and Class Members immediately after learning of the 2024 Cellular Data Breach and then by failing to provide Plaintiff and Class Members sufficient information regarding the breach.

104. Further, through its failure to provide timely and clear notification of the 2024 Cellular Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

105. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures. In addition to their duties under common law, Defendants had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred because of Defendants' failure to observe these duties, including the loss of privacy, significant risk of identity theft, and Plaintiff's and Class Members' overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

106. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and Class Members to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

107. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendants' duty in this regard.

108. AT&T gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

109. AT&T violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

110. AT&T breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' PII, and by failing to provide prompt notice without reasonable delay.

111. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

112. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

113. The harm that occurred because of the 2024 Cellular Data Breach is the type of harm the FTC Act was intended to guard against.

114. AT&T breached its duties to Plaintiff and Class Members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

115. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2024 Cellular Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in their continued possession; (g) future costs in terms of time, effort, and money that will be expended as a result of the 2024 Cellular Data Breach for the remainder of the lives of Plaintiff and other Class Members; and (h) the diminished value of Plaintiff's and Class Members' PII; (i) the diminished value of AT&T's services Plaintiff and other Class Members paid for and received; and/or (j) the actual and attempted sale of Plaintiff's and Class Members' PII on the dark web.

116. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Count II -Invasion of Privacy

117. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

118. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

119. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

120. Defendants allowed unauthorized and unknown third parties access to and acquire the PII of Plaintiff and Class Members because it failed to protect and implement adequate security measures for the PII.

121. The unauthorized access to, acquisition of, and/or viewing of the PII of Plaintiff and Class Members by unauthorized third parties is highly offensive to a reasonable person.

122. Defendants' willful and reckless conduct which enabled the theft and disclosure of Plaintiff's and Class Members' sensitive and confidential personal information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

123. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendants as part of obtaining services from Defendants, but privately and with the intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that their disclosure of private facts in the form of PII would be kept private and would not be disclosed without their authorization and the disclosure of their PII through the 2024 Cellular Data Breach was wholly without their consent, and in violation of state and federal law.

124. The 2024 Cellular Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interests in solitude or seclusion,

either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

125. AT&T acted with a knowing state of mind when it permitted the 2024 Cellular Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

126. Because AT&T acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

127. As a proximate result of the above acts and omissions of AT&T, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

128. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant scan be accessed, acquired, and viewed by unauthorized persons for years to come.

129. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff or Class members.

Count III - Unjust Enrichment

130. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

131. Plaintiff and Class Members paid for Defendants' products and services.

132. As Defendants collected, maintained, and stored the PII of Plaintiff and Class Members, AT&T had knowledge of the monetary benefits it received on behalf of the Plaintiff and Class Members.

133. The funds that Plaintiff and Class Members paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

134. Defendants failed to implement, or failed to effectively implement, the adequate data security practices, procedures, and programs to secure sensitive PII, as evidenced by the 2024 Cellular Data Breach.

135. As a result of Defendants' failure to implement the data security practices, procedures, and programs required to adequately secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the funds paid by Plaintiff and Class Members paid that Defendants reasonably and contractually should have expended on data security measures to secure their PII.

136. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII for which they paid.

137. As a direct and proximate result of Defendants' decision to profit rather than provide adequate security, and Defendants' resultant disclosures of Plaintiff's and the Class Members' PII, Plaintiff and Class Members suffered, and continue to suffer, substantial injuries, including in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, actual harm and/or a continuing increased risk of harm.

Count IV - Breach of Implied Contract

138. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

139. When Plaintiff and Class Members provided their PII to Defendants in connection with seeking wireless voice, messaging, and data services, they entered into implied contracts in which AT&T agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII.

140. Defendants required Plaintiff and Class Members to provide PII to receive wireless voice, messaging, and/or data services.

141. AT&T affirmatively represented that it collected and stored the PII of Plaintiff and Class Members using proper means.

142. Based on Defendants' representations and the requirements of AT&T for the use of its goods and services, Plaintiff and Class Members accepted Defendants 'offers and provided Defendants with their PII.

143. Plaintiff and Class Members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised.

144. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

145. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII.

146. AT&T also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: (i) representing that it would maintain adequate data privacy

and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections of Defendants' information systems; and (iii) failing to disclose to Plaintiff and Class Members at the time they provided their PII that Defendants' data security system and protocols failed to meet applicable legal and industry standards.

147. The 2024 Cellular Data Breach was a reasonably foreseeable consequence of Defendants' acts and omissions in breach of these contracts.

148. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2024 Cellular Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in their continued possession; (g) future costs in terms of time, effort, and money that will be expended as a result of the 2024 Cellular Data Breach for the remainder of the lives of Plaintiff and other members of the proposed class; and (h) the diminished value of Plaintiff's and Class Members' PII; (i) the diminished value of

AT&T's services Plaintiff and other members of the proposed class paid for and received; and/or (j) the actual and attempted sale of Plaintiff's and Class Members' PII on the dark web.

Count V Breach of Confidence

149. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

150. At all relevant times, AT&T was fully aware of the confidential nature of Plaintiff's and Class Members' PII.

151. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by promises and expectations that Plaintiff and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties.

152. Plaintiff and Class Members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect the PII and not permit the PII to be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties. Plaintiff and Class Members also provided their PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect their PII, such as following basic principles of protecting their networks and data systems.

153. Defendants voluntarily received, in confidence, Plaintiff's and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, disclosed to, or viewed by the public or any unauthorized third parties.

154. Due to Defendants' failure to prevent, detect, and avoid the 2024 Cellular Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was accessed by, acquired

by, disclosed to, or viewed by unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

155. But for Defendants' failure to maintain and protect Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, disclosed to, or viewed by unauthorized third parties. Defendants'2024 Cellular Data Breach was the direct and legal cause of the misuse of Plaintiff's and Class Members' PII, as well as the resulting damages.

156. As a direct and proximate result of Defendants' actions and omissions, Plaintiff and Class Members have suffered damages as alleged herein.

157. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Plaintiff's and Class Members' PII. AT&T knew its data systems and protocols for accepting and securing Plaintiff's and Class Members' PII had security and other vulnerabilities that placed Plaintiff's and Class Members' PII in jeopardy.

158. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2024 Cellular Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in AT&T's possession and is subject to further unauthorized

disclosures so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the 2024 Cellular Data Breach for the remainder of the lives of Plaintiff and other Class Members; and (g) the diminished value of Plaintiff's and Class Members' PII; (h) the diminished value of AT&T's services Plaintiff and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiff's and Class Members' PII on the dark web.

Count VI Breach of Contract

159. Plaintiff incorporates by reference the allegations in paragraphs 1 through 87 above as though fully set forth herein.

160. Plaintiff and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts with Defendant.

161. Upon information and belief, these agreements include Defendants' affirmative obligations to keep its customers' sensitive PII private and secure.

162. Upon information and belief, these contracts included promises made by Defendants that expressed and/or manifested intent that the contracts were made to benefit Plaintiff and Class Members primarily and directly, as Defendants' business is not only to provide products and services for Plaintiff and the Class, but also to safeguard the PII with which it was entrusted in connection with providing such products and services.

163. Upon information and belief, Defendants 'representations required Defendants to implement the necessary security measures to protect Plaintiff's and Class Members' PII. Defendants materially breached its contractual obligations to protect Plaintiff's and Class

Members' PII when that information was accessed and exfiltrated as part of the 2024 Cellular Data Breach.

164. The 2024 Cellular Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of Plaintiff's and Class Members' contracts.

165. As a direct and proximate result of the 2024 Cellular Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and loss of control of their PII, in addition to the present risk of suffering additional damages and out-of-pocket expenses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

B. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the public as requested herein, including, but not limited to:

   a. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   b. Ordering Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

d. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

e. Ordering Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

f. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

g. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

h. Requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

i. Ordering that Defendants segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, unauthorized third parties cannot gain access to other portions of Defendants' systems;

j. Prohibiting Defendants from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

k. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

l. Ordering that Defendants conduct regular database scanning and securing checks;

m. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

n. Ordering Defendants to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Defendants' information network for both internal and external threats, and assess whether monitoring tools are appropriately configured, tested, and updated; and

D. Ordering Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying

information to third parties, as well as the steps affected individuals must take to protect themselves;

E. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

F. An award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined; An award of punitive damages; and

G. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and an award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted, this 16th day of July, 2024.

HERMAN JONES LLP

/s/ Serina M. Vash

Serina M. Vash
(NYS Bar No. 2773448)
HERMAN JONES LLP
153 Central Avenue #131
Westfield, New Jersey 07090
Tel: (862) 250-3930
svash@hermanjones.com

John C. Herman*
(Ga. Bar No. 348370)
3424 Peachtree Road, N.E., Suite 1650
Atlanta, Georgia 30326
Telephone: (404) 504-6500
Facsimile: (404) 504-6501
jherman@hermanjones.com
(*to be admitted *pro hac vice*)

Counsel for Plaintiff